



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

7590

07/10/2008

Joseph S Tripolis
Thomson Multimedia Licensing Inc
PO Box 5312
Princeton, NJ 08540

EXAMINER

DAVIS, ZACHARY A

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 07/10/2008

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/743,653

03/14/2001

Ahmet Mursit Eskicioglu

RCA 89131

7330

TITLE OF INVENTION: CONDITIONAL ACCESS SYSTEM FOR BROADCAST DIGITAL TELEVISION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1440	\$0	\$0	\$1440	10/10/2008

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail

**Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

7590

07/10/2008

Joseph S Tripolis
Thomson Multimedia Licensing Inc
PO Box 5312
Princeton, NJ 08540

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/743,653	03/14/2001	Ahmet Mursit Eskicioglu	RCA 89131	7330

TITLE OF INVENTION: CONDITIONAL ACCESS SYSTEM FOR BROADCAST DIGITAL TELEVISION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1440	\$0	\$0	\$1440	10/10/2008

EXAMINER	ART UNIT	CLASS-SUBCLASS
DAVIS, ZACHARY A	2137	380-231000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/147; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

1

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

2

3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.111. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/743,653

03/14/2001

Ahmet Mursit Eskicioglu

RCA 89131

7330

7590

07/10/2008

Joseph S Tripolis
Thomson Multimedia Licensing Inc
PO Box 5312
Princeton, NJ 08540

EXAMINER

DAVIS, ZACHARY A

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 07/10/2008

Determination of Patent Term Extension under 35 U.S.C. 154 (b)

(application filed after June 7, 1995 but prior to May 29, 2000)

The Patent Term Extension is 0 day(s). Any patent to issue from the above-identified application will include an indication of the 0 day extension on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Extension is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability

Application No.

09/743,653

Examiner

Zachary A. Davis

Applicant(s)

ESKICIOGLU ET AL.

Art Unit

2137

- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERIT IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment received 09 August 2007.
2. ☒ The allowed claim(s) is/are 1-4, 6 and 15-17.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. A petition to revive the present application under 37 CFR 1.137(b) and the required response were received on 09 August 2007. The petition was granted 12 December 2007.
2. By the above response, Claim 1 has been amended. No claims have been added or canceled. Claims 7-14 were previously withdrawn from further consideration as drawn to a nonelected species. Claims 1-4, 6, and 15-17 are currently under consideration in the present application.

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.
4. The application has been amended as follows:

IN THE CLAIMS:

Please **CANCEL Claims 7-14**.

5. This application is in condition for allowance except for the presence of claims 7-14 directed to a species non-elected without traverse. Accordingly, claims 7-14 have been cancelled, as noted above.

Response to Arguments

6. Applicant's arguments, see pages 5-8 of the present response, filed 09 August 2007, with respect to Claims 1-4, 6, and 15-17 have been fully considered and are persuasive. The rejection of Claims 1-4, 6, and 15-17 has been withdrawn.

7. The Examiner notes that Applicant appears to have mischaracterized both the prior art and the present invention in portions of the arguments noted above. In particular, Applicant states that "the use of individual private keys, as taught by Wasilewski, requires that each broadcast stream sent to each individual set top box be separately encrypted and transmitted" (page 6 of the present response). However, this is a misapprehension of the Wasilewski reference. While Wasilewski does disclose that each set top unit has its own private key (see column 8, lines 37-39), Wasilewski does not disclose encrypting the broadcast stream for each individual set top unit with the corresponding public keys. Instead, each program (or broadcast stream) is encrypted using randomly generated keys called control words and each control word is encrypted with another randomly generated key referred to as a multi-session key (MSK), and each of these encryptions is performed using a symmetric algorithm (see column 7, line 64-column 8, line 30, for example). The MSKs are then each encrypted for the individual set top units using their respective public keys (column 8, lines 31-47, for example); however, the symmetric keys (MSKs and control words) are the same for each set top unit (see also column 22, line 61-column 23, line 32) and therefore the

programs ("broadcast streams") do not need to be encrypted individually for each set top unit. Only the symmetric keys are encrypted with each public key; the programs are not encrypted with each public key, in contrast to Applicant's assertions.

Applicant further characterizes the present invention in which "multiple consumers receive the same broadcast, which is encrypted with the same public key" (page 7 of the present response). However, this is not what is claimed or described in the present specification; instead, the access information associated with the transmitted event (i.e. the broadcast) is what is encrypted with the private key (see Claim 1). This access information is similar to the control words and MSKs in Wasilewski (see above). The description of the invention in the present specification also does not disclose multiple consumers receiving a broadcast encrypted with the same public key, but rather that an "entitlement message" is encrypted with the public key, and the message includes the key to decrypt the keys used to scramble the broadcast program (see page 2, lines 29-33 of the present specification; see also page 15, lines 1-7, where the symmetric keys encrypted under the public key are explicitly referred to as control words, as also described in Wasilewski).

However, Applicant's argument that neither Wasilewski nor Kudelski discloses a private key shared among a plurality of subscribers (see pages 5-8 of the present response) is persuasive, and therefore the rejection has been withdrawn.

Allowable Subject Matter

8. Claims 1-4, 6, and 15-17 are allowed.
9. The following is an examiner's statement of reasons for allowance:

Independent Claim 1 is directed to a method for managing access to a restricted transmitted event, where access information for the event is received from a service provider encrypted under a public key shared by multiple service providers. The access information is decrypted using the corresponding private key, which is shared by multiple subscribers. The conditional access module verifies whether the cost of the event, included in the access information, is less than a pre-stored cash reserve, and if so, the event is received and descrambled. The closest prior art, Kudelski and Wasilewski, as previously cited, disclose a similar method, including a public key system for encrypting access information, where the public key is shared by a plurality of service providers, and also verifying whether a received cost of the event is less than a pre-stored cash reserve, and receiving and descrambling the scrambled transmitted event. However, neither Kudelski nor Wasilewski, alone or in combination, teach or suggest that the private key is shared among a plurality of subscribers. Therefore, the claims are allowable over the cited prior art.

The Examiner acknowledges Applicant's remarks in the present specification, noting that the use of more than a single shared private key would increase the security of the system (see page 2, lines 12-14, and page 15, lines 9-16, of the present specification).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Messing, US Patent 6745327, discloses a system in which multiple users share a private key on a network computer. This reference does not qualify as prior art to the present application, but has been included for completeness.
- b. Benardeau et al, US Patent 6904522, discloses a system in which devices may share the same private key if the devices are distributed in different regions. This reference does not qualify as prior art to the present application, but has been included for completeness.
- c. Srivastava, US Patent 7181014, discloses a method in which a broadcast group has a private key shared by each group member. This reference does not qualify as prior art to the present application, but has been included for completeness.
- d. Zeanah et al, US Patent 7249344, discloses a system with a cryptographic management component holding shared secret or private keys.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137